Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 287 (2004) 155–160

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Note

Character sums and MacWilliams identities☆

Dae San Kim[a], Dong Chan Kim[b]

[a]*Department of Mathematics, Sogang University, Sinsu-dong 1, Mapo-gu, Seoul 121-742, Republic of Korea*
[b]*Department of Mathematics, Sogang University, Seoul 121-742, Republic of Korea*

Received 1 May 2003; accepted 24 June 2004

Abstract

We show that certain character sums are intimately connected with MacWilliams identities for linear poset codes as well as usual linear codes. We also illustrate in some two poset codes that this method gives much shorter proofs than the ones using discrete Poisson summation formula.

MSC: primary 11L03; 94B60; secondary 94B05

Keywords: Character sum; MacWilliams(-type) identity; Poset code

1. Character sums and MacWilliams identity

Character sums have diverse applications in many areas such as number theory, optics, coding theory and cryptography. Here, we demonstrate that certain character sums are intimately connected with the classical MacWilliams identity for linear codes and the more recent MacWilliams-type identities for linear codes on posets (cf. [3,4]).

Let C be a linear code of length n over the finite field $\mathbb{F}_q$ with q elements, and let $\{A_i\}_{i=0}^{i=n}$, $\{B_i\}_{i=0}^{i=n}$ respectively be the Hamming weight distributions of C and its dual code $C^{\perp}$. Then the classical MacWilliams identity for C is equivalent to (1.1) in the following (cf. [6, pp. 88]). The proof of the next theorem is based on (1.3) and simple change of order of summation, in contrast to the usual proof exploiting discrete Poisson summation formula.

Theorem 1.1. *Let C, $\{A_i\}_{i=0}^{i=n}$, $\{B_i\}_{i=0}^{i=n}$ be as above. Then we have*

$$B_i = \frac{1}{|C|} Q_i(C; n, q) \quad (i = 0, 1, \ldots, n). \tag{1.1}$$

Here we put

$$Q_i(C; n, q) := \sum_{j=0}^{n} A_j P_i(j; n, q) = \sum_{u \in C} P_i(w(u); n, q), \tag{1.2}$$

E-mail addresses: dskim@ccs.sogang.ac.kr (D.S. Kim), taiji96@math.sogang.ac.kr (D.C. Kim).
☆ This work was supported by Grant No. R01-2002-000-00083-0(2003) from the Basic Research Program of the Korea Science and Engineering Foundation.

0012-365X/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.06.007

where

$$P_i(x;n,q)=\sum_{l=0}^{i}(-1)^l(q-1)^{i-l}\binom{x}{l}\binom{n-x}{i-l}\quad(i=0,1,2,\ldots,n)$$

are the Krawtchouk polynomials and $w(u)$ denotes the Hamming weight of the vector $u\in\mathbb{F}_q^n$.

Proof. Let λ be a nontrivial additive character of $\mathbb{F}_q$. Then, as is well-known [5, p. 74], for any vector $u\in\mathbb{F}_q^n$ we have

$$\sum_{w(v)=i}\lambda(u\cdot v)=P_i(w(u);n,q). \tag{1.3}$$

In view of (1.2–3), RHS of (1.1) equals

$$\frac{1}{|C|}\sum_{u\in C}\sum_{w(v)=i}\lambda(u\cdot v)=\sum_{w(v)=i}\frac{1}{|C|}\sum_{u\in C}\lambda(u\cdot v)=B_i, \tag{1.4}$$

as

$$\frac{1}{|C|}\sum_{u\in C}\lambda(u\cdot v)=\begin{cases}1 & \text{if } v\in C^{\perp},\\ 0 & \text{if } v\notin C^{\perp}.\end{cases}\qquad\square$$

Remark 1.2. From (1.1) and (1.4),

$$\sum_{u\in C}\sum_{w(v)=i}\lambda(u\cdot v)=Q_i(C;n,q)\quad(i=0,1,\ldots,n). \tag{1.5}$$

2. Quick review of poset codes

Here we briefly review the notion of poset-weight, poset-distance and a poset code (a code on a poset) introduced by Brualdi et al. [1]. Let P denote a poset with the partial order $\leqslant$ on the underlying set

$$[n]=\{1,2,\ldots,n\}$$

of coordinate positions of vectors in $\mathbb{F}_q^n$. Then the P-weight $w_P(u)$ of $u=(u_1,u_2,\ldots,u_n)$ in $\mathbb{F}_q^n$ is defined to be

$$w_P(u)=|\langle\mathrm{Supp}(u)\rangle|,$$

where $\langle\mathrm{Supp}(u)\rangle$ denotes the smallest ideal containing the support of u defined by $\mathrm{Supp}(u)=\{i\,|\,1\leqslant i\leqslant n, u_i\neq 0\}$ (recall a subset I of $[n]$ is an ideal if $a\in I$ and $b<a\Rightarrow b\in I$). Then $d_P(u,v)=w_P(u-v)$ is a metric (called P-metric) on $\mathbb{F}_q^n$. Let $\mathbb{F}_q^n$ be endowed with the P-metric induced by the poset P. Then a (linear) code $C\subseteq\mathbb{F}_q^n$ is called a (linear) code of length n over $\mathbb{F}_q$ on P (or a P-code of length n over $\mathbb{F}_q$). The P-weight enumerator of such a C is defined by

$$W_{C,P}(x,y)=\sum_{x\in C}x^{n-w_P(u)}y^{w_P(u)}=\sum_{i=0}^{n}A_{i,P}x^{n-i}y^i,$$

where, for $A_{i,P}=|\{u\in C\,|\,w_P(u)=i\}|$, $\{A_{i,P}\}_{i=0}^{i=n}$ is called the P-weight distribution of C.

Remark 2.1. If P is an antichain, then the P-weight enumerator of C specializes to the Hamming weight enumerator of C given by

$$W_C(x,y)=\sum_{x\in C}x^{n-w(u)}y^{w(u)}=\sum_{i=0}^{n}A_ix^{n-i}y^i.$$

3. Character sums and MacWilliams identities for certain posets

Let C be a linear code of length n over $\mathbb{F}_q$ on a poset P, and let $\{B_{i,P}\}_{i=0}^{i=n}$ be the P-weight distribution of the dual P-code $C^{\perp}$ of C. Just as in (1.4), we have the simple identity

$$\frac{1}{|C|}\sum_{u\in C}\sum_{w_P(v)=i}\lambda(u\cdot v)=\sum_{w_P(v)=i}\frac{1}{|C|}\sum_{u\in C}\lambda(u\cdot v)=B_{i,P}. \tag{3.1}$$

In [3,4], MacWilliams-type identities for linear codes on the poset $P=n_1\mathbf{1}\oplus n_2\mathbf{1}\oplus\cdots\oplus n_t\mathbf{1}$ and $(n,n-1,j)$-poset were obtained (cf. Sections 3.1 and 3.2). These generalize the MacWilliams-type identity for linear codes on a simple poset in [2] which are special cases of the posets just mentioned. The discrete Poisson summation formula was used in deriving both of them. Instead here we use the character sum identity (3.1), and derive similar results to (1.5) that are equivalent to the MacWilliams-type identities just mentioned. This method gives much shorter proofs than the original ones.

3.1. Derivation of MacWilliams identity for $P=n_1\mathbf{1}\oplus n_2\mathbf{1}\oplus\cdots\oplus n_t\mathbf{1}$

Let $n_1,n_2,\ldots,n_t$ be positive integers with $n=n_1+n_2+\cdots+n_t$. Then, in this subsection, $P=n_1\mathbf{1}\oplus n_2\mathbf{1}\oplus\cdots\oplus n_t\mathbf{1}$ is the poset whose underlying set and order relation are given by

$$[n]=n_1\mathbf{1}\cup n_2\mathbf{1}\cup\cdots\cup n_t\mathbf{1},$$

$$(n_i\mathbf{1}=\{n_1+\cdots n_{i-1}+1,\cdots,n_1+\cdots n_{i-1}+n_i\}),$$

$$a<b\Leftrightarrow a\in n_i\mathbf{1},b\in n_j\mathbf{1},\quad \text{for some } i,j \text{ with } i<j,$$

where $n_0=0$.

In view of the poset structure of P, it is natural to write

$$\mathbb{F}_q^n=\mathbb{F}_q^{n_1}\oplus\mathbb{F}_q^{n_2}\oplus\cdots\oplus\mathbb{F}_q^{n_t},$$

$$u=(u_1,u_2,\ldots,u_t),\quad u_i\in\mathbb{F}_q^{n_i},\quad \text{for } u\in\mathbb{F}_q^n,$$

so that u_i is the ith block of coordinates of u. Then the usual inner product of $u=(u_1,u_2,\ldots,u_t)$ and $v=(v_1,v_2,\ldots,v_t)$ is given by

$$u\cdot v=\sum_{i=1}^{t}u_i\cdot v_i.$$

If s is the largest integer with $u_s\neq 0$, for $u=(u_1,u_2,\ldots,u_t)\in\mathbb{F}_q^n$, then

$$w_P(u)=w(u_s)+\sum_{i=1}^{s-1}n_i. \tag{3.2}$$

Let $\pi_j:C\to\mathbb{F}_q^{n_j}$ $(1\leqslant j\leqslant t)$ be the projection of C into the jth block of coordinates, $\rho_j=\pi_1\oplus\pi_2\oplus\cdots\oplus\pi_j:C\to\mathbb{F}_q^{n_1}\oplus\mathbb{F}_q^{n_2}\oplus\cdots\oplus\mathbb{F}_q^{n_j}$ $(1\leqslant j\leqslant t)$, and let $\rho_0:C\to\{0\}$. Then, after simple modification and using (1.2), the MacWilliams-type identity in [4, Theorem 1.1] can be written as

$$W_{C^{\perp},P}(x,y)=x^n+\frac{1}{|C|}\sum_{j=1}^{t}\sum_{i=1}^{n_j}q^{\sum_{l=1}^{j-1}n_l}|\ker\rho_j|Q_i(j)x^{\sum_{l=j}^{t}n_l-i}\,y^{\sum_{l=1}^{j-1}n_l+i}, \tag{3.3}$$

where $Q_i(j)=Q_i(\pi_j(\ker\rho_{j-1});n_j,q)$.

In view of (3.1), (3.3) is equivalent to (3.4).

Theorem 3.1. *For $1\leqslant j\leqslant t$ and $1\leqslant i\leqslant n_j$,*

$$\sum_{u\in C}\sum_{w_P(v)=\sum_{l=1}^{j-1}n_l+i}\lambda(u\cdot v)=q^{\sum_{l=1}^{j-1}n_l}|\ker\rho_j|Q_i(\pi_j(\ker\rho_{j-1});n_j,q). \tag{3.4}$$

Proof. First note that, in view of (3.2), for $v=(v_1, v_2, \dots, v_t) \in \mathbb{F}_q^n$

$$w_P(v)=\sum_{l=1}^{j-1} n_l + i \quad \Leftrightarrow \quad v_{j+1}=\cdots=v_t=0 \quad \text{and} \quad w(v_j)=i.$$

Thus the inner sum in LHS of (3.4) is seen to be equal to

$$\prod_{l=1}^{j-1} \sum_{v_l \in \mathbb{F}_q^{n_l}} \lambda(u_l \cdot v_l) \times \sum_{w(v_j)=i} \lambda(u_j \cdot v_j) = \prod_{l=1}^{j-1} q^{n_l} \delta_{u_l,0} \times P_i(w(u_j); n_j, q), \tag{3.5}$$

where we used (1.3), and $\delta_{u_l,0}=1$ if $u_l=0$ and $\delta_{u_l,0}=0$ otherwise. Thus, from (3.5) and (1.2), the LHS of (3.4) is

$$\begin{aligned} q^{\sum_{l=1}^{j-1} n_l} \sum_{u \in \ker \rho_{j-1}} P_i(w(u_j); n_j, q) &= q^{\sum_{l=1}^{j-1} n_l} |\ker \rho_j| \sum_{u_j \in \pi_j(\ker \rho_{j-1})} P_i(w(u_j); n_j, q) \\ &= q^{\sum_{l=1}^{j-1} n_l} |\ker \rho_j| Q_i(\pi_j(\ker \rho_{j-1}); n_j, q), \end{aligned}$$

as we wanted. □

3.2. Derivation of MacWilliams identity for $(n, n-1, j)$-poset

In this subsection, $P=P(j)$ denotes the poset whose underlying set and only order relation are respectively given by

$$[n]=\{1, 2, \dots, n-j+1, n-j+2, \dots, n\}$$

and

$$1<i, \quad \text{for } i=2, 3, \dots, n-j+1.$$

Here $1 \leqslant j \leqslant n-1$, and one notes that $P=P(j)$ is a poset with n elements and with $n-1$ maximal elements and j minimal elements, i.e., an"$(n, n-1, j)$-poset".

In accordance with the poset structure of $P=P(j)$, we write

$$\mathbb{F}_q^n = \mathbb{F}_q \oplus \mathbb{F}_q^{n-j} \oplus \mathbb{F}_q^{j-1},$$

$$\begin{aligned} &u=(u_1, \dots, u_n)=(u_1, u', u'')=(u_1, \tilde{u}),\\ &u'=(u_2, \dots, u_{n-j+1}), \quad u''=(u_{n-j+2}, \dots, u_n),\\ &\tilde{u}=(u_2, \dots, u_{n-j+1}, u_{n-j+2}, \dots, u_n). \end{aligned}$$

Let $\phi_1 : \mathbb{F}_q^n \to \mathbb{F}_q$ $(u \mapsto u_1)$, $\phi_2 : \mathbb{F}_q^n \to \mathbb{F}_q^{n-j}$ $(u \mapsto u')$, $\phi_3 : \mathbb{F}_q^n \to \mathbb{F}_q^{j-1}$ $(u \mapsto u'')$, respectively, be the projection of $\mathbb{F}_q^n$ onto the first coordinate, the next $n-j$ coordinates and the last $j-1$ coordinates. Then we put $\pi_i=\phi_i|_C$, for $i=1, 2, 3$.

Remark 3.2. For $j=1$, we agree that $\pi_3 : C \to \{0\}$. In particular, $\ker \pi_3 = C$, and we understand that $W_{\pi_3(C)}(x, y)=1$.

Also, let $\eta_1=\phi_1 \oplus \phi_2 : \mathbb{F}_q^n \to \mathbb{F}_q \oplus \mathbb{F}_q^{n-j}$, $\eta_2=\phi_2 \oplus \phi_3 : \mathbb{F}_q^n \to \mathbb{F}_q^{n-j} \oplus \mathbb{F}_q^{j-1}$ be the projections of $\mathbb{F}_q^n$ onto the first $n-j+1$ coordinates and the last $n-1$ coordinates, respectively. Then we set

$$\rho_1=\eta_1|_C=\pi_1 \oplus \pi_2, \quad \rho_2=\eta_2|_C=\pi_2 \oplus \pi_3.$$

As was noted in (2.7) of [3], one easily sees that, for $v \in \mathbb{F}_q^n$,

$$w_P(v)=\begin{cases} w(v) & \text{if } v \in (\mathbb{F}_q^n \backslash \ker \phi_1) \cup \ker \eta_1, \\ w(v)+1 & \text{if } v \in \ker \phi_1 \backslash \ker \eta_1. \end{cases} \tag{3.6}$$

We note that the sum over $u \in C$ of the polynomial $\Phi_u(x, y; j-1)$ given in (2.12) of [3] is nothing other than

$$|\ker \pi_3| W_{\pi_3(C)}(x+y, x-y),$$

with the convention $W_{\pi_3(C)}(x,y)=1$ for $j=1$ as in the above remark. Then, working with q-ary codes instead of binary ones and using Hamming weight enumerators rather than P-weight ones, in our notation Theorem 2.1 in [3] can be translated into

$$W_{C^\perp,P}(x,y)=\frac{1}{|C|}\left\{x^{n-j}(x-y)|\ker\pi_3|W_{\pi_3(C)}(x+(q-1)y,x-y)\right.$$
$$\left.+qyW_{\rho_2(\ker\pi_1)}(x+(q-1)y,x-y)\right\} \tag{3.7}$$

(cf. [3, (2.11–12)]).

In view of (1.2–3) or (1.5), it is natural to agree that

$$Q_i(*;m,q)=0 \quad \text{if } i<0 \text{ or } i>m.$$

With this in mind and using the notation in (1.2), (3.7) can be rewritten as

$$\begin{aligned}W_{C^\perp,P}(x,y)&=\frac{1}{|C|}\left\{\sum_{i=0}^{j-1}|\ker\pi_3|Q_i(\pi_3(C);j-1,q)x^{n-i}y^i-\sum_{i=1}^{j}|\ker\pi_3|Q_{i-1}(\pi_3(C);j-1,q)x^{n-i}y^i\right.\\&\left.+\sum_{i=1}^{n}qQ_{i-1}(\rho_2(\ker\pi_1);n-1,q)x^{n-i}y^i\right\}\\&=\frac{1}{|C|}\sum_{i=0}^{n}\{|\ker\pi_3|Q_i(\pi_3(C);j-1,q)-|\ker\pi_3|Q_{i-1}(\pi_3(C);j-1,q)\\&+qQ_{i-1}(\rho_2(\ker\pi_1);n-1,q)\}x^{n-i}y^i.\end{aligned}$$

In view of (3.1), this is equivalent to (3.8).

Theorem 3.3. *For* $0\leqslant i\leqslant n$,

$$\sum_{u\in C}\sum_{w_P(v)=i}\lambda(u\cdot v)=|\ker\pi_3|Q_i(\pi_3(C);j-1,q)-|\ker\pi_3|Q_{i-1}(\pi_3(C);j-1,q)$$
$$+qQ_{i-1}(\rho_2(\ker\pi_1);n-1,q). \tag{3.8}$$

Proof. Invoking (3.6), the LHS of (3.8) can be written as S_1+S_2, with

$$S_1=\sum_{u\in C}\sum_{v\in\ker\eta_1\ \text{with}\ w(v)=i}\lambda(u\cdot v)-\sum_{u\in C}\sum_{v\in\ker\eta_1\ \text{with}\ w(v)=i-1}\lambda(u\cdot v),$$
$$S_2=\sum_{u\in C}\sum_{v\in\mathbb{F}_q^n\setminus\ker\phi_1\ \text{with}\ w(v)=i}\lambda(u\cdot v)+\sum_{u\in C}\sum_{v\in\ker\phi_1\ \text{with}\ w(v)=i-1}\lambda(u\cdot v).$$

Now,

$$\begin{aligned}S_1&=|\ker\pi_3|\sum_{u''\in\pi_3(C)}\sum_{v''\in\mathbb{F}_q^{j-1}\ \text{with}\ w(v'')=i}\lambda(u''\cdot v'')-|\ker\pi_3|\sum_{u''\in\pi_3(C)}\sum_{v''\in\mathbb{F}_q^{j-1}\ \text{with}\ w(v'')=i-1}\lambda(u''\cdot v'')\\&=|\ker\pi_3|Q_i(\pi_3(C);j-1,q)-|\ker\pi_3|Q_{i-1}(\pi_3(C);j-1,q).\end{aligned}$$

On the other hand,

$$S_2=\sum_{u\in\ker\pi_1}\sum_{v\in\mathbb{F}_q^n\setminus\ker\phi_1\ \text{with}\ w(v)=i}\lambda(u\cdot v)+\sum_{u\in C\setminus\ker\pi_1}\sum_{v\in\mathbb{F}_q^n\setminus\ker\phi_1\ \text{with}\ w(v)=i}\lambda(u\cdot v)$$
$$+\sum_{u\in C}\sum_{v\in\ker\phi_1\ \text{with}\ w(v)=i-1}\lambda(u\cdot v). \tag{3.9}$$

The middle sum in (3.9) is

$$\sum_{(u_1,\tilde{u})\in C\setminus\ker\pi_1}\sum_{v_1\in\mathbb{F}_q^\times}\lambda(u_1v_1)\sum_{\tilde{v}\in\mathbb{F}_q^{n-1}\text{ with }w(\tilde{v})=i-1}\lambda(\tilde{u}\cdot\tilde{v})=-\sum_{(u_1,\tilde{u})\in C\setminus\ker\pi_1}\sum_{\tilde{v}\in\mathbb{F}_q^{n-1}\text{ with }w(\tilde{v})=i-1}\lambda(\tilde{u}\cdot\tilde{v})$$

(noting that $\sum_{v_1\in\mathbb{F}_q^\times}\lambda(u_1v_1)=-1,$ since $u_1\neq 0$)

$$=-\sum_{u\in C\setminus\ker\pi_1}\sum_{v\in\ker\phi_1\text{ with }w(v)=i-1}\lambda(u\cdot v)$$

$$=-\sum_{u\in C}\sum_{v\in\ker\phi_1\text{ with }w(v)=i-1}\lambda(u\cdot v)+\sum_{u\in\ker\pi_1}\sum_{v\in\ker\phi_1\text{ with }w(v)=i-1}\lambda(u\cdot v).$$

So,

$$S_2=\sum_{u\in\ker\pi_1}\sum_{v\in\mathbb{F}_q^n\setminus\ker\phi_1\text{ with }w(v)=i}\lambda(u\cdot v)+\sum_{u\in\ker\pi_1}\sum_{v\in\ker\phi_1\text{ with }w(v)=i-1}\lambda(u\cdot v)$$

$$=(q-1)\sum_{\tilde{u}\in\rho_2(\ker\pi_1)}\sum_{\tilde{v}\in\mathbb{F}_q^{n-1}\text{ with }w(\tilde{v})=i-1}\lambda(\tilde{u}\cdot\tilde{v})+\sum_{\tilde{u}\in\rho_2(\ker\pi_1)}\sum_{\tilde{v}\in\mathbb{F}_q^{n-1}\text{ with }w(\tilde{v})=i-1}\lambda(\tilde{u}\cdot\tilde{v})$$

$$=qQ_{i-1}(\rho_2(\ker\pi_1);n-1,q).\qquad\square$$

References

[1] R.A. Brualdi, J. Graves, K.M. Lawrence, Codes with a poset metric, Discrete Math. 147 (1995) 57–72.
[2] J.N. Gutiérrez, H. Tapia-Recillas, A MacWilliams identity for poset-codes, Congr. Numer. 133 (1998) 63–73.
[3] Y. Jang, J. Park, On a MacWilliams type identity and a perfectness for a binary linear $(n, n-1, j)$-poset codes, Discrete Math. 265 (2003) 85–104.
[4] D.S. Kim, J.G. Lee, A MacWilliams-type identity for linear codes on weak order, Discrete Math. 262 (2003) 181–194.
[5] J.H. van Lint, Introduction to Coding Theory, third ed., Springer, Berlin, 1999.
[6] V.S. Pless, W.C. Huffman, Handbook of Coding Theory, vol. I, Elsevier Science B. V., Amsterdam, 1998.